

DOCKET NO.: 265501US6PCT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Hisato SHIMA, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP04/11475

INTERNATIONAL FILING DATE: August 10, 2004

FOR: COMMUNICATION PROCESSING APPARATUS, COMMUNICATION CONTROLLING  
METHOD AND COMPUTER PROGRAM

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119**  
**AND THE INTERNATIONAL CONVENTION**

Commissioner for Patents  
Alexandria, Virginia 22313

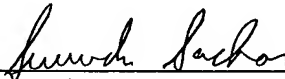
Sir:

In the matter of the above-identified application for patent, notice is hereby given that  
the applicant claims as priority:

<b><u>COUNTRY</u></b>	<b><u>APPLICATION NO</u></b>	<b><u>DAY/MONTH/YEAR</u></b>
Japan	2003-291971	12 August 2003

Certified copies of the corresponding Convention application(s) were submitted to the  
International Bureau in PCT Application No. PCT/JP04/11475. Receipt of the certified  
copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been  
acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,  
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



\_\_\_\_\_  
Gregory J. Maier  
Attorney of Record  
Registration No. 25,599  
Surinder Sachar  
Registration No. 34,423

Customer Number

**22850**

(703) 413-3000  
Fax No. (703) 413-2220  
(OSMMN 08/03)

**BEST AVAILABLE COPY**

PCT/JP 2004/011475

日本国特許庁  
JAPAN PATENT OFFICE

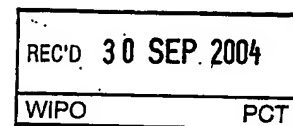
11.08.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2003年 8月12日

出願番号  
Application Number: 特願2003-291971  
[ST. 10/C]: [JP 2003-291971]

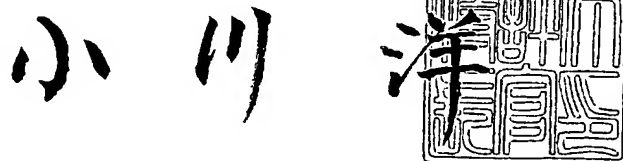


出願人  
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 9月16日

特許庁長官  
Commissioner,  
Japan Patent Office



出証番号 出証特2004-3083680

【書類名】 特許願  
【整理番号】 0390562803  
【提出日】 平成15年 8月12日  
【あて先】 特許庁長官殿  
【国際特許分類】 H04L 9/00  
【発明者】  
    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社内  
    【氏名】 嶋 久登  
【発明者】  
    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社内  
    【氏名】 中野 雄彦  
【特許出願人】  
    【識別番号】 000002185  
    【氏名又は名称】 ソニー株式会社  
【代理人】  
    【識別番号】 100093241  
    【弁理士】  
    【氏名又は名称】 宮田 正昭  
    【電話番号】 03-5541-7577  
【選任した代理人】  
    【識別番号】 100101801  
    【弁理士】  
    【氏名又は名称】 山田 英治  
    【電話番号】 03-5541-7577  
【選任した代理人】  
    【識別番号】 100086531  
    【弁理士】  
    【氏名又は名称】 澤田 俊夫  
    【電話番号】 03-5541-7577  
【手数料の表示】  
    【予納台帳番号】 048747  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9904833

**【書類名】 特許請求の範囲****【請求項 1】**

ネットワークを介した通信処理を実行する通信処理装置であり、

通信先デバイスの識別情報を異なるデータ処理レベルで複数取得し、取得した複数の識別情報の照合を行い、該照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する構成を有することを特徴とする通信処理装置。

**【請求項 2】**

通信先デバイスから受信する少なくとも 1 つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信する構成であることを特徴とする請求項 1 に記載の通信処理装置。

**【請求項 3】**

前記通信処理装置は、

通信先デバイスから受信する識別情報として、OSI 参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信し、これらの複数の識別情報の照合を行う構成であることを特徴とする請求項 1 に記載の通信処理装置。

**【請求項 4】**

通信先デバイスから受信する識別情報は、IEEE 1394 規格によって規定されたノードユニーク ID であることを特徴とする請求項 1 に記載の通信処理装置。

**【請求項 5】**

前記通信処理装置は、

通信先デバイスから受信する識別情報として、通信先デバイスの PHY 通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信し、これらの複数の識別情報の照合を行う構成であることを特徴とする請求項 1 に記載の通信処理装置。

**【請求項 6】**

通信先デバイスから受信する識別情報は、ブルートゥース通信規格によって規定されたブルートゥースデバイス・アドレスであることを特徴とする請求項 1 に記載の通信処理装置。

**【請求項 7】**

前記通信処理装置は、

通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づくデータを受信し、これらの複数のブルートゥースデバイス・アドレスの照合を行う構成であることを特徴とする請求項 1 に記載の通信処理装置。

**【請求項 8】**

ネットワークを介した通信処理を実行する通信制御方法であり、

通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する識別情報取得ステップと、

取得した複数の識別情報の照合を実行する照合処理ステップと、

照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、

を有することを特徴とする通信制御方法。

**【請求項 9】**

前記識別情報取得ステップにおいて通信先デバイスから受信する少なくとも 1 つの識別

情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信することを特徴とする請求項 8 に記載の通信制御方法。

【請求項 10】

前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、OSI 参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信するステップであり、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする請求項 8 に記載の通信制御方法。

【請求項 11】

通信先デバイスから受信する識別情報は、IEEE 1394 規格によって規定されたノードユニーク IDであることを特徴とする請求項 8 に記載の通信制御方法。

【請求項 12】

前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスの PHY 通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信するステップであり、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする請求項 8 に記載の通信制御方法。

【請求項 13】

通信先デバイスから受信する識別情報は、ブルートゥース通信規格によって規定されたブルートゥースデバイス・アドレスであることを特徴とする請求項 8 に記載の通信制御方法。

【請求項 14】

前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づくデータを受信し、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする請求項 8 に記載の通信制御方法。

【請求項 15】

ネットワークを介した通信処理を実行するコンピュータ・プログラムであり、通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する識別情報取得ステップと、

取得した複数の識別情報の照合を実行する照合処理ステップと、

照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、

を有することを特徴とするコンピュータ・プログラム。

## 【書類名】明細書

【発明の名称】通信処理装置、および通信制御方法、並びにコンピュータ・プログラム

## 【技術分野】

## 【0001】

本発明は、通信処理装置、および通信制御方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、例えばホームネットワーク等のローカルネットワーク内に接続された機器と、インターネット等の外部ネットワークに接続された機器とを区別可能とした認証を実行して通信を行うことにより、例えばホームネットワーク内でのみ利用の許容されたコンテンツの外部流出など、コンテンツ不正利用処理などを排除可能とした通信処理装置、および通信制御方法、並びにコンピュータ・プログラムに関する。

## 【背景技術】

## 【0002】

昨今のデータ通信ネットワークの普及に伴い、家庭内においても家電機器やコンピュータ、その他の周辺機器をネットワーク接続し、各機器間での通信を可能とした、いわゆるホームネットワークが浸透しつつある。ホームネットワークは、ネットワーク接続機器間で通信を行なうことにより各機器のデータ処理機能を共有したり、機器間でコンテンツの送受信を行なう等、ユーザに利便性・快適性を提供するものであり、今後、ますます普及することが予測される。

## 【0003】

しかし、一方、この種のネットワークでは、不正アクセスに対する対策を考慮することも必要となる。ホームネットワーク内の機器、例えばサーバ等には私的なコンテンツや有料コンテンツ等の著作権管理を要求されるコンテンツが格納されることも多い。

## 【0004】

このようなホームネットワーク内のサーバに格納されたコンテンツや秘密情報は、例えば、インターネットを介した外部からのアクセスによって不正に取得される可能性がある。このような不正アクセスを許容すると、秘密漏洩を生じさせることにもなり、また、コンテンツ著作権の管理の観点からも重要な問題である。

## 【0005】

このように、映画や音楽など著作権の管理が必要なコンテンツをネットワークを通じて伝送する場合、そのコンテンツ伝送範囲は利用が許可された範囲、例えばホームネットワーク内のデバイス間に留めることが求められるが、近年のインターネットの普及に伴い、インターネットを介したコンテンツの不正な伝送が行われ、問題になっている。

## 【発明の開示】

## 【発明が解決しようとする課題】

## 【0006】

本発明は、このような状況に鑑みてなされたものであり、ホームネットワーク等の特定のローカルネットワーク内の機器と、インターネット等の外部ネットワークに接続された機器とを明確に区別する認証構成を実現したものである。コンテンツ等のデータ転送の際には、認証処理を実行し、ホームネットワーク等のローカルネットワークの接続機器であることの確認を行う構成とすることで、コンテンツの不正流出、秘密情報の漏洩等の防止を可能とした通信処理装置、および通信制御方法、並びにコンピュータ・プログラムを提供することを目的とする。

## 【課題を解決するための手段】

## 【0007】

本発明の第1の側面は、

ネットワークを介した通信処理を実行する通信処理装置であり、

通信先デバイスの識別情報を異なるデータ処理レベルで複数取得し、取得した複数の識別情報の照合を行い、該照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する構成を有することを特徴とする通

信処理装置にある。

【0008】

さらに、本発明の通信処理装置の一実施態様において、通信先デバイスから受信する少なくとも1つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信する構成であることを特徴とする。

【0009】

さらに、本発明の通信処理装置の一実施態様において、前記通信処理装置は、通信先デバイスから受信する識別情報として、OSI参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信し、これらの複数の識別情報の照合を行う構成であることを特徴とする。

【0010】

さらに、本発明の通信処理装置の一実施態様において、通信先デバイスから受信する識別情報は、IEEE1394規格によって規定されたノードユニークIDであることを特徴とする。

【0011】

さらに、本発明の通信処理装置の一実施態様において、前記通信処理装置は、通信先デバイスから受信する識別情報として、通信先デバイスのPHY通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信し、これらの複数の識別情報の照合を行う構成であることを特徴とする。

【0012】

さらに、本発明の通信処理装置の一実施態様において、通信先デバイスから受信する識別情報は、ブルートゥース通信規格によって規定されたブルートゥースデバイス・アドレスであることを特徴とする。

【0013】

さらに、本発明の通信処理装置の一実施態様において、前記通信処理装置は、通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づくデータを受信し、これらの複数のブルートゥースデバイス・アドレスの照合を行う構成であることを特徴とする。

【0014】

さらに、本発明の第2の側面は、  
ネットワークを介した通信処理を実行する通信制御方法であり、  
通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する識別情報取得ステップと、  
取得した複数の識別情報の照合を実行する照合処理ステップと、  
照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、  
を有することを特徴とする通信制御方法にある。

【0015】

さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップにおいて通信先デバイスから受信する少なくとも1つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信することを特徴とする。

【0016】

さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、OSI参照モデルにおける物理層またはデ

ータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信するステップであり、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする。

【0017】

さらに、本発明の通信制御方法の一実施態様において、通信先デバイスから受信する識別情報は、IEEE1394規格によって規定されたノードユニークIDであることを特徴とする。

【0018】

さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスのPHY通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信するステップであり、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする。

【0019】

さらに、本発明の通信制御方法の一実施態様において、通信先デバイスから受信する識別情報は、ブルートゥース通信規格によって規定されたブルートゥースデバイス・アドレスであることを特徴とする。

【0020】

さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づくデータを受信し、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする。

【0021】

さらに、本発明の第3の側面は、ネットワークを介した通信処理を実行するコンピュータ・プログラムであり、通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する識別情報取得ステップと、取得した複数の識別情報の照合を実行する照合処理ステップと、照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、を有することを特徴とするコンピュータ・プログラムにある。

【0022】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0023】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基くより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【0024】

本発明の構成によれば、ホームネットワーク等のネットワークに対して、インターネット等の外部ネットワークに接続された機器からアクセスされた場合、そのアクセスが外部



機器からか内部のローカルネットワーク内の機器からであるかを明確に判別することが可能となり、本発明の判定を伴う認証を実行することによりローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの漏洩、流出を未然に防止することが可能となる。

#### 【0025】

本発明の構成では、通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する。例えば少なくとも1つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信する。また、OS参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信し、これらの複数の識別情報の照合を行う。このように、複数の異なるデータ処理レベルで取得された識別情報の照合を行い、照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かが確実に判定され、ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの外部に対する漏洩、流出を未然に防止することが可能となる。

#### 【0026】

本発明の構成によれば、IEEE1394規格におけるノードユニークIDや、ブルートゥース規格におけるブルートゥースデバイス・アドレスを適用した比較照合が可能であり、既存の通信において設定済みの識別情報を利用可能となる。

【発明を実施するための最良の形態】

#### 【0027】

以下、図面を参照しながら本発明の通信処理装置、および通信制御方法、並びにコンピュータ・プログラムの詳細について説明する。

#### 【0028】

まず、図1を参照して、本発明の適用可能なネットワーク構成例について説明する。図1は、例えば特定ユーザの家等に構築されたホームネットワーク100等のローカルエリアネットワーク、すなわち内部ネットワークであり、パーソナルコンピュータ(PC)101、102、TV103、ハードディスクレコーダ104、PDA105等の様々な情報処理装置がホームネットワーク100を介してデータ送受信を行う。

#### 【0029】

たとえば、PC101、102、あるいはハードディスクレコーダ104をコンテンツ提供サーバとし、TV103、PDA105をクライアントとして、クライアントがサーバの格納コンテンツをネットワークを介して取得し、クライアントのディスプレイ、スピーカを利用してコンテンツ出力を行う。

#### 【0030】

ホームネットワーク100は、有線、無線等いずれかのネットワークであり、各接続機器は、通信パケットをネットワークを介して送受信する。

#### 【0031】

図1において、ホームネットワーク100は、インターネット等の外部ネットワーク120に接続されている。外部ネットワーク120にもPC121、携帯電話122、ポータブル再生プレーヤ123等の各種の通信処理装置が接続される。ホームネットワーク100内の通信処理装置と外部ネットワーク120の通信処理装置とは、外部ネットワーク120およびホームネットワーク100を介して通信が可能となる。

#### 【0032】

外部ネットワーク120およびホームネットワーク100によって構成される内部ネットワークの間には、外部ネットワーク120と内部ネットワーク間の通信を可能とするデータ処理、例えばホームネットワーク内のデータ通信パケットであるIEEE1394パケットと、外部ネットワークでの転送パケットであるイーサネットパケット、IPパケットの変換などを実行する通信サーバ110が接続される。

## 【0033】

外部ネットワーク120に接続されたPC121、携帯電話122、ポータブル再生プレーヤ123等の各種の通信処理装置は、通信サーバ110を介してホームネットワーク100内のサーバ、例えばPC101、102、ハードディスクレコーダ103等にアクセスし、これらの装置に格納されたコンテンツを取得してPC121、携帯端末122、再生プレーヤ123等においてコンテンツ出力を行うことが可能となる。

## 【0034】

ただし、これらのコンテンツ取得を不特定のクライアントに許容することは、コンテンツの著作権、秘密漏洩等の問題から好ましいことではない。従って、機器間の通信においては、後段で説明する本発明の認証シーケンスに従った認証処理を実行し、内部ネットワーク内のデータが外部に不正に流出するのを防止する構成としている。この詳細処理構成については後述する。

## 【0035】

図1に示す各ネットワーク接続機器としての通信処理装置のハードウェア構成例について図2を参照して説明する。

## 【0036】

CPU(Central Processing Unit)201は、ROM(Read Only Memory)202、またはHDD(Hard Disk Drive)204等に記憶されているプログラムに従って、各種の処理を実行し、データ処理手段、あるいは通信制御処理手段として機能する。RAM(Random Access Memory)203には、CPU201が実行するプログラムやデータが適宜記憶される。CPU201、ROM202、およびRAM203、HDD204は、バス205を介して相互に接続されている。

## 【0037】

バス205には、入出力インタフェース206が接続されており、この入出力インタフェース206には、例えば、ユーザにより操作されるキーボード、スイッチ、ボタン、あるいはマウス等により構成される入力部207、ユーザに各種の情報を提示するLCD、CRT、スピーカ等により構成される出力部208が接続される。さらに、データ送受信手段として機能する通信部209、さらに、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどのリムーバブル記録媒体211を装着可能で、これらのリムーバブル記録媒体211からのデータ読み出しあるいは書き込み処理を実行するドライブ210が接続される。通信部209は、例えばIEEE1394規格に従った通信、あるいはBluetooth規格に従った通信処理の可能な構成を持つ。

## 【0038】

なお、図2に示す構成は、図1に示すネットワーク接続機器の一例としての一般的なPCの構成を示すものであるが、ネットワーク接続機器はPCに限らず、図1に示すように携帯電話、PDA等の携帯通信端末、その他の様々な電子機器、通信処理装置によって構成することが可能である。従って、それぞれの機器固有のハードウェア構成を持つことが可能であり、そのハードウェアに従った処理を実行する。

## 【0039】

本発明の通信処理装置において実行する機器間の通信においては、まず機器間の認証処理を実行し、認証処理の結果、通信相手が同一のホームネットワーク等のローカルネットワーク接続された機器であることが確認された場合に、コンテンツ等のデータ転送を許容する。認証処理においては、通信先デバイスの識別情報を異なるデータ処理レベルで複数取得し、取得した複数の識別情報の照合を行い、該照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるかを判定する処理を実行する。

## 【0040】

1つの具体例としては、例えば通信機器の識別子(ID)をOSI参照モデルにおける物理層やデータリンク層での通信と、ネットワーク層以上の例えばアプリケーション層での通信においてそれぞれ受領し、この2つのIDを比較する処理を行う。以下、本発明に

従った認証処理の具体例について、IEEE 1394 規格に従った通信を行う構成例と、ブルートゥース規格に従った通信を行う構成例について説明する。

#### 【0041】

(1) IEEE 1394 規格に従った通信を行う構成例

ホームネットワーク等のローカルネットワークに接続された通信処理装置は、IEEE 1394 データインターフェイスを備え、IEEE 1394 方式に従ったデータ転送を実行する。IEEE 1394 データインターフェイスは、例えば SCSI などよりもデータ転送レートが高速であり、所要のデータサイズを周期的に送受信することが保証されるアイソクロナス (Isochronous) 通信が可能である。このため、IEEE 1394 データインターフェイスは、AV (Audio/Video) などのストリームデータをリアルタイムで転送するのに有利となる。

#### 【0042】

IEEE 1394 によるデータ伝送方式には、上述のアイソクロナス (Isochronous) 通信方式と、非同期で通信するアシンクロナス (Asynchronous) 通信方式が存在する。一般に、アイソクロナス (Isochronous) 通信方式はデータの送受信に用いられ、アシンクロナス (Asynchronous) 通信方式は各種制御コマンドの送受信に用いられる。1本のケーブルを使用して、これら2種類の通信方式によって送受信を行うことができる。

#### 【0043】

各種デジタルAV機器やパーソナルコンピュータ装置等の電子機器を、IEEE (Institute of Electrical Engineers) 1394 等のデジタルデータインターフェイス規格に従ったデータバスを介して相互に接続することで、機器間でデータを送受信できるようにしたデータ伝送システムが構築される。

#### 【0044】

このようなAVシステムでは、いわゆるリモート制御も可能となる。例えば、データバスを介してディスク記録再生装置とパーソナルコンピュータが接続されると、ディスク記録再生装置に対する記録再生、更には記録ソースの編集などに関する操作をパーソナルコンピュータ装置側での操作によって行うことも可能となる。

#### 【0045】

本発明の通信処理装置としてのIEEE 1394 対応機器の構成について図3を用いて説明する。

#### 【0046】

送受信部301の内部には、データ処理手段としてPHY-IC303、LINK-IC304、ネットワーク通信部 (IEEE 1394 制御マイコン) 305を有する。なお、PHY-IC303とLINK-IC304をまとめてPHY通信部とみなす。

#### 【0047】

PHY-IC303は、物理層の電氣的インタフェースを受け持ち、LINK-IC304からのパラレルデータをシリアル変換し、IEEE 1394 規格の電気信号を発生し、逆にIEEE 1394 規格信号をシリアルデータに戻しパラレルデータとしてLINK-IC304に送信する。また、PHY-IC303は、バス (ケーブル) の状態認識、バスの初期化、アービトラージ処理などを実行する。すなわち、PHY-IC303は、IEEE 1394 規格のプロトコルに従って、IEEE 1394 端子302を介してIEEEシリアルバス310との間の通信を制御し、IEEE 1394シリアルバス310から供給されるデジタルビデオデータやデジタルオーディオデータがパケット化されたアイソクロナスパケット、または制御信号がパケット化されたアシンクロナスパケットをLINK-IC304に供給する。PHY-IC303はまた、LINK-IC304から供給されるアイソクロナスパケットやアシンクロナスパケットを、IEEE 1394シリアルバス310に出力する。

#### 【0048】

LINK-IC304は、データリンク層を受け持ち、送信データパケットのPHY-

IC303への送出、PHY-IC303受信パケットのトランザクション／アプリケーション層への送出を実行する。すなわち、PHY-IC303から供給されるアシンクロナスパケットを、IEEE1394制御マイコン305が解読できるデジタル信号（コマンド）に変換し、IEEE1394制御マイコン305に供給したり、IEEE1394制御マイコン305から供給されるデジタル信号をアシンクロナスパケットに変換し、PHY-IC303に供給する。LINK-IC304はまた、PHY-IC303から供給されるアイソクロナスパケットをデジタル信号に変換したり、機器から入力される主データ（例えば、デジタルビデオデータ、デジタルオーディオデータ）を、アイソクロナスパケットに変換し、PHY-IC303に供給する。

**【0049】**

ネットワーク通信部（IEEE1394制御マイコン）305は、LINK-IC304から供給されたコマンドを機器制御マイコン306に転送するとともに、そのコマンドに対応するレスポンスを生成し、LINK-IC304に出力する。

**【0050】**

機器制御マイコン306は、ネットワーク通信部（IEEE1394制御マイコン）305から供給されたコマンドに対応して、機器内部の回路（図示せず）を制御し、各種の処理を実行させる。

**【0051】**

LINK-IC304は、EPROMなどのメモリ321が接続ないし内蔵され、メモリ321に書き込まれたIDを読み取ることができる。図では、メモリ321をLINK-IC304に内蔵した例を示している。

**【0052】**

メモリ321に格納されるIDは、グローバルユニーク（Global Unique）な値を用いるものとする。また、LINK-IC304、メモリ321は、耐タンパ構成を持つパッケージとして構成され、IDや通信内容の改ざんの困難性を高めた構成を持つ。IDの改ざんを困難にする方法の具体例としては、例えば、LINK-IC304とIDの格納メモリ321を1つのICで構成することや、複数のICで構成される場合はIC間の通信を保護するために通信路を暗号化したり、あるいはICをBGAパッケージにして、配線を基板の内層に埋め込んで信号にアクセスできなくするといった構成とするなどの各種構成が適用可能である。

**【0053】**

ネットワーク通信部（IEEE1394制御マイコン）305は、LINK-IC304を通じて他のネットワーク接続機器のネットワーク通信部と通信を行うことができる。また、各ネットワーク通信部は、自身のLINK-IC304経由でIDを読み取ることができる。

**【0054】**

以上のように構成される1394対応機器は、IEEE1394シリアルバス310を介して、他の各接続機器とデータ送受信、通信を実行することができる。

**【0055】**

例えばIEEE1394対応機器としてのVTRに所定の機能を実行させるとき、IEEE1394バスに接続されたパーソナルコンピュータ（PC）は、その機能の実行を指令する、例えば、再生、記録、巻戻しなどのAV/Cコマンド（以下、これらをまとめてAV/Cコマンドと称する）を、IEEE1394シリアルバスを介してVTRに伝送する。

**【0056】**

VTRは、AV/Cコマンドを受信すると、それに対応した処理を実行するとともに、所定のレスポンスをAV/Cコマンドの送信元である、パーソナルコンピュータ（PC）に出力する。

**【0057】**

図4を参照して、ネットワーク接続機器間の通信の際に実行する認証処理シーケンスに

ついて説明する。

【0058】

図4に示すフローは機器Aが、通信を行おうとする機器Bが適切な通信相手であることを確認し、通信の可否を制御するフローである。すなわち、機器Aは、機器Bが機器Aと同一のホームネットワーク内の内部ネットワーク接続機器であるか、インターネット等の外部ネットワークに接続された機器であるかを判別する。

【0059】

まず、機器Aは、ステップS111において、相手機器BのPHY通信部に対するコマンドとして、ID要求コマンド1を送る。機器BのPHY通信部は、ステップS112において、ID要求を受けると、ステップS113において、PHY通信部の処理として自身のIDを読み出して、ステップS114において、機器Aに対して返送する。

【0060】

機器Aは、ステップS115において、機器BのPHY通信部からのIDを受信し、受信IDを、後の処理のために記憶しておく。以上の通信は、OSI参照モデルのデータリンク層以下で実施されるものとし、ブリッジやルーターを介さないネットワーク接続機器間の通信においてのみ可能なものとする。

【0061】

次に機器Aは、ステップS116において、機器Bのネットワーク通信部に対するコマンドとして、ID要求コマンド2を送る。機器Bのネットワーク通信部は、ステップS117において、ID要求コマンド2を受けると、機器Bのネットワーク通信部は、ステップS118において、自身のPHY通信部経由でメモリに格納されたIDを読み出して、ステップS119において機器Aに対して読み出したIDを返送する。この通信は、OSI参照モデルのネットワーク層以上で実施されるものとし、ブリッジやルーターを介した機器とも通信可能なものとする。なお、この通信で得たIDを以後、ID'とする。

【0062】

機器Aは、ステップS120において、機器Bのネットワーク通信部からID'を受信すると、ステップS121において、受信したID'が、先に機器BのPHY通信部から受信したIDと一致するか確認する。

【0063】

一致した場合、すなわちID=ID'が成立する場合は、ステップS122に進み、相手機器との通信を許可し、引き続き通信を行う。一方、一致しない場合、すなわちID≠ID'が成立しない場合は、ステップS123に進み、以後の通信を禁止する。

【0064】

機器間の通信は、通信途上での改ざんやなりすましを防止するため、両方の機器が共有する秘密データに基づいて保護された状態で行われることも考えられる。例えば暗号化したり、通信内容に対する電子署名や鍵付きハッシュ値を送るなどの手段が適用されうる。

【0065】

図5に、ネットワーク通信部からのID送信の際に、特定の正当な機器のみが保持する秘密情報としての鍵を適用した暗号処理やハッシュ値生成処理によって取得IDのデータ処理を実行し、暗号化データあるいはハッシュ値としてのIDを送信する構成とした例について説明する。

【0066】

機器Aは、ステップS201において、相手機器BのPHY通信部に対するコマンドとして、ID要求コマンド1を送る。機器BのPHY通信部は、ID要求を受けると、ステップS202において、PHY通信部の処理として自身のIDを読み出して、ステップS203において、機器Aに対して返送する。

【0067】

機器Aは、機器BのPHY通信部からのIDを受信し、受信IDを、後の処理のために記憶しておく。次に、ステップS204において、機器Bのネットワーク通信部に対するコマンドとして、ID要求コマンド2を送る。機器Bのネットワーク通信部は、ID要求

コマンド2を受けると、ステップS205において、自身のPHY通信部経由でメモリに格納されたIDを読み出して、機器Aと機器Bが共有する秘密データ、すなわち暗号処理鍵やハッシュ値生成鍵を適用し、読み出したIDに対する暗号処理鍵を適用した暗号化、あるいはハッシュ値生成鍵を適用したハッシュ値生成処理を行い、生成したデータをステップS206において、機器Aに送信する。

#### 【0068】

機器Aは、受信したID2が例えば暗号化データである場合は、機器Bと共有する鍵に基づいて復号処理を実行し、復号結果として得られたID2と先にPHY通信部から受信したID1とを照合比較する。両者が一致すれば、ID1を送信した機器とID2を送信した機器とは同一であり、PHY通信部の通信が実行可能な内部ネットワーク接続機器との通信が実行されていると判定し、その後の通信、例えばコンテンツ提供を行う。ID1とID2が一致しない場合は、ID1を送信した機器とID2を送信した機器とは同一でない。すなわち、ID1は、PHY通信部の通信が実行可能な内部ネットワーク接続機器が機器Aに提供し、ID2はインターネット等、外部ネットワークに接続された機器が機器Aに送信してきたものと判定し、不正な外部からのアクセスが行われていると判定し、その後の通信、例えばコンテンツ提供を実行することなく、通信を停止する。

#### 【0069】

また、機器Aは、受信したID2が例えばハッシュ値である場合は、先にPHY通信部から受信したID1に対して、機器Bと共有するハッシュ値生成鍵に基づいてハッシュ値を生成し、結果として得られたID1に基づくハッシュ値と、機器Bのネットワーク通信部から受信したID2に基づくハッシュ値とを照合比較する。両者が一致すれば、ID1を送信した機器とID2を送信した機器とは同一であり、PHY通信部の通信が実行可能な内部ネットワーク接続機器との通信が実行されていると判定し、その後の通信、例えばコンテンツ提供を行う。不一致の場合は、上述と同様、外部からの不正アクセスであると判定し、その後の通信、例えばコンテンツ提供を実行することなく、通信を停止する。

#### 【0070】

本発明の上述した認証シーケンスを実行することにより、ローカルネットワークに接続された機器と、外部ネットワーク接続機器とを区別することが可能となり、外部ネットワークを介した不正アクセスを排除することができる。

#### 【0071】

すなわち、図6(a)に示すように、ローカルバス上に接続された機器A411と機器B412がある場合、機器Aは、上述した認証シーケンスにおいて機器Bから受信するIDはID1=ID2となる。しかし、図6(b)に示すように、機器A421が外部ネットワークに接続された機器C422と接続して、上述の認証シーケンスを実行した場合、機器A421はローカル接続した機器X431のPHY通信部からID1を受信し、機器C422のネットワーク通信部からID2を受信することになる。この場合ID1=ID2は成立せず、機器A421は、外部ネットワーク接続機器からのアクセスであると判定し、通信を終了することができる。

#### 【0072】

なお、上記処理において、機器間で送受信するIDは、IEEE1394規定において定められているノードユニークIDを適用することが可能である。

#### 【0073】

IEEE1394では、コンフィグレーションROMに64ビットのノードユニークIDを持つことが規定されている。このIDは、IEEE1394で規定されたアシンクロナス通信によって直接参照することができる。通常ノードユニークIDの情報は、IEEE1394のICだけで処理が完結する。一方、IEEE1394のICを実装する装置において、そのIC以外のIC、例えばCPUからIEEE1394のIC経由でノードユニークIDを読み取ることができれば、上述した直接的な参照方法以外の方法でIDを受け渡すこともできる。例えば上述したように2つの機器が共有する秘密鍵を用いた暗号化データとして送受信することができる。

## 【0074】

IEEE1394の機器同士で、本発明の処理を実行する場合、通信相手を1394のローカルバス内の機器に限定するため、1394の10ビットのバスIDは全ビット1とし、ブリッジを経由した異なるバス上の機器とは通信を行わないことを前提とする。

## 【0075】

しかし、先に説明した図6(b)のように、機器Xが機器Cに、また機器Yが機器Aになりすますことで、ローカルバスを越えた通信を行うことも可能である。これを防ぐために機器Aは、通信相手のコンフィグレーションROMにアクセスし、ノードユニークIDを直接参照するとともに、前述の別のプロトコルによってもIDを取得する。この場合、機器Aは、ローカルバス上にいる機器XのコンフィグレーションROMを参照することしかできず、機器XのノードユニークIDを参照する一方、機器Aと秘密鍵を共有する機器は、機器Cなので、機器X、Y経由で機器CのIDを取得することになる。これらのIDは一致しないことになり、結果として機器Aは、機器Cがローカルバス上に存在しないことを検知し、中継された通信を防止することができる。

## 【0076】

(2) ブルートゥース規格に従った通信を行う構成例

次に、ホームネットワーク等のローカルネットワークに接続された通信処理装置が、ブルートゥース規格に従った通信を行う構成例について説明する。

## 【0077】

近年、近距離間の無線通信手段としてブルートゥース(Bluetooth)が注目されており、様々な対応機器が開発、販売されている。

## 【0078】

このブルートゥースによる無線通信システムは、従来のIrDA(Infrared Data Association)のような赤外線通信方式と比較して、指向性がなく、透過性が高いなどの長所を有している。従って、IrDAなどの指向性が強い通信を利用する際には、通信を行わせる機器同士を適切に向かい合わせる必要があったが、ブルートゥースなどの通信システムでは、そのような位置の制約は不要となる。

## 【0079】

ブルートゥースの規格に関しては、Bluetooth SIG Inc.によって管理されており、その詳細については、Bluetooth SIG Inc.から誰でも入手することが可能であるが、例えば、ブルートゥースを用いた通信においては、通信を制御するマスタと呼ばれる機器から、周囲に存在する機器を検出するための機器検出メッセージがブロードキャスト送信される。

## 【0080】

そして、マスタは、この機器検出メッセージを受信した機器(スレーブ)から送信されてきた応答メッセージによって、周囲に存在する機器、すなわち通信可能な機器を検出することができる。

## 【0081】

また、マスタは、検出した機器の中から、特定の機器との間で通信を確立する場合、応答メッセージに含まれるそれぞれの機器の識別情報に基づいて機器を特定し、その通信を確立する。

## 【0082】

ブルートゥースにおいては、そのような機器を識別する情報としてブルートゥースデバイス・アドレスと呼ばれる情報が個々の機器に付与されており、それぞれの機器に対して固有(一義的)であることから、機器の管理等、様々な処理に利用される。

## 【0083】

図7を参照して、ブルートゥース規格に準拠した無線通信ネットワークとしてのピコネットを形成して、ピコネットを形成した通信処理装置間で、相互に各種のデータを送受信する通信システムの構成例について説明する。

## 【0084】

前述したように、ブルートゥースを用いた通信においては、通信を制御するマスタと呼

ばれる機器と、マスタを介した通信を実行する複数のスレーブと呼ばれる機器によって形成されるネットワーク（ピコネット）において通信が実行される。ブルートゥースにおいては、各機器を識別する情報としてブルートゥースデバイス・アドレスが個々の機器に設定され、ブルートゥースデバイス・アドレスに基づいて、通信対象の特定がなされる。

#### 【0085】

マスタとスレーブからなるピコネットにおいては、1つのマスタに対して、最大7つのスレーブが属することができる。同一のピコネットに属する全ての機器は、周波数軸（周波数ホッピングパターン）と時間軸（タイムスロット）が同期している状態にある。

#### 【0086】

図7においては、パーソナルコンピュータ（PC）501がマスタとして設定され、その他の機器、パーソナルコンピュータ（PC）521、携帯電話522、PDA（Personal Digital Assistants）523、ビデオカメラ524が各々スレーブとして設定された構成例を示している。

#### 【0087】

これらの1つのマスタと複数のスレーブによって構成されるピコネットは、他の外部ネットワークと接続しない独立したネットワーク（アドホックモード）として存在することも、あるいはインターネット、あるいは他のピコネット等、他のネットワークにマスタを介して接続した構成（インフラストラクチャモード）とすることも可能である。

#### 【0088】

このピコネットは、パーソナルエリアネットワーク（PAN）とも呼ばれ、スレーブの各々は、PANU（PANユーザ：PAN User）と呼ばれる。また、他のネットワークと接続された構成（インフラストラクチャモード）におけるマスタは、ピコネットを構成するスレーブ間の通信パケットの中継、すなわちパケット交換処理を実行するとともに、外部接続ネットワークとのパケット交換も実行し、NAP（Network Access Point）と呼ばれる。一方、他の外部ネットワークと接続しない独立したネットワーク（アドホックモード）におけるマスタは、ピコネットを構成するスレーブ間の通信パケットの中継を行ない、GN（Group Ad-hoc Network）と呼ばれる。

#### 【0089】

ブルートゥースにおいては、無線通信で送受信されるデータや、その通信手順に関して、サービス毎に取り決めたプロファイルと呼ばれる仕様が策定されており、このプロファイルに従って、各機器が提供できるサービスが表わされている。PAN（Personal Area Network）プロファイルでは、ピコネットにおけるスレーブ間の通信方法が規定されており、PANプロファイルに基づいて構成されたピコネットに属する機器は、そのピコネットを1つのネットワークとして各種のデータを送受信する。

#### 【0090】

図7に示すマスタとしてのパーソナルコンピュータ（PC）501、スレーブとしてのパーソナルコンピュータ（PC）521、携帯電話522、PDA523、ビデオカメラ524は、それぞれブルートゥースモジュールを内蔵しており、ブルートゥース規格に準拠した無線通信により、相互に各種のデータを送受信できるようになされている。

#### 【0091】

マスタ、スレーブを構成する各機器には、ブルートゥース規格に準拠した無線通信を実行するためのブルートゥースモジュールが備えられる。具体的には、無線周波数として、2.4GHzのISM帯を使用した時分割多重方式を採用し、ISM帯において周波数ホッピングスペクトラム拡散通信による無線通信を行なうためのモジュールである。

#### 【0092】

ブルートゥースモジュールの具体的構成例について、図8を参照して説明する。CPU601は、ROM602に格納されている制御プログラムをRAM603に展開し、ブルートゥースモジュール600の全体の動作を制御する。CPU601は、データ処理手段、あるいは通信制御処理手段として機能する。これらのCPU601乃至RAM603は、バス605を介して相互に接続されており、このバス605には、また、フラッシュメモ



メモリ 604 が接続されている。

【0093】

フラッシュメモリ 604 には、例えば、ピコネットを構成するマスタ、スレーブそれぞれのブルートゥースデバイスに設定されているブルートゥースデバイス名、および、それぞれのブルートゥースデバイスに対して固有なブルートゥースデバイス・アドレスなどが記憶されている。

【0094】

このブルートゥースデバイス・アドレスは、48ビットの識別子であり、それぞれのブルートゥースデバイスに対して固有（一義的）であることから、ブルートゥースデバイスの管理に関する様々な処理に利用される。

【0095】

例えば、ピコネット内同期を確立するためには、全てのスレーブがマスタの周波数ホッピングパターンに関する情報を取得している必要があり、この周波数ホッピングパターンは、マスタのブルートゥースデバイス・アドレスに基づいてスレーブにより算出されるようになされている。

【0096】

より詳細には、ブルートゥースデバイス・アドレスは、図9に示すように、24ビットのロー・アドレスパート（LAP: Low Address Part）と、8ビットのアップパー・アドレスパート（UAP: Upper Address Part）と、そして残りの16ビットのノン・シグニフィカントアドレスパート（NAP: Non-significant Address Part）とそれぞれ区分された構成を持ち、周波数ホッピングパターンの算出には、LAP全体の24ビットとUAPの下位4ビットからなる28ビットが用いられる。

【0097】

スレーブの各々は、ピコネット内同期を確立するための「呼び出し（Page）」により取得したマスタのブルートゥースデバイス・アドレスの、上述した28ビットの部分と、同様にマスタから通知されたブルートゥースクロックに基づいて、周波数ホッピングパターンを算出することができる。

【0098】

図8の説明に戻る。フラッシュメモリ 604 には、ピコネット内同期確立後に、通信相手のブルートゥースデバイスを認証したり、送信するデータを暗号化したりするためのリンクキーなどが記憶され、必要に応じてCPU 601 に提供される。

【0099】

入出力インタフェース 606 は、CPU 601 からの指示に基づく供給データ、およびベースバンド制御部 607 から供給されてきたデータの入出力を管理する。

【0100】

ベースバンド制御部 607 は、トランシーバ 608 の制御、リンクの制御、パケットの制御、論理チャネルの制御、セキュリティの制御などの各種の制御、および誤り訂正符号化、復号化、或いはデータのランダム化などの処理を行い、入出力インタフェース 606 から供給されてきたデータをアナログ変換してトランシーバ 608 に出力するとともに、トランシーバ 608 から供給されてきた信号をデジタル変換して得られたデータを入出力インタフェース 606 に出力する。

【0101】

トランシーバ 608 は、GFSK (Gaussian Frequency Shift Keying) 変調部、GFSK 復調部、スペクトラム拡散部、逆スペクトラム拡散部、或いはホッピングシンセサイザ部等より構成され、ベースバンド制御部 607 から供給されてきた信号に各種の処理を施し、アンテナ 609 に出力するとともに、アンテナ 609 から供給されてきた信号に各種の処理を施し、得られた信号をベースバンド制御部 607 に出力する。

【0102】

トランシーバ 608 を構成する GFSK 変調部は、ベースバンド制御部 607 から供給されてきたデータの高域成分をフィルタにより制限し、1 次変調として周波数変調を行い

、取得したデータをスペクトラム拡散部に出力する。スペクトラム拡散部は、上述したようにLAP全体の24ビットとUAPの下位4ビットからなる28ビットにより算出され、ホッピングシンセサイザ部から通知される周波数ホッピングパターンに基づいて搬送周波数を切り替え、供給されてきたデータに対してスペクトラム拡散を施した後に得られた信号をアンテナ609に出力する。ブルートゥースにおいては、スペクトラム拡散部は、625 $\mu$ 秒毎に周波数をホッピングさせて、データを送信するようになされている。

#### 【0103】

また、トランシーバ608を構成する逆スペクトラム拡散部は、ホッピングシンセサイザ部から通知される周波数ホッピングパターンに基づいて受信周波数をホッピングさせ、例えば、通信相手のスレーブから送信されてきた信号を取得する。また、逆スペクトラム拡散部は、取得した信号を逆スペクトラム拡散し、通信相手のスレーブからの信号を再生した後に得られた信号をGFSK復調部に出力する。GFSK復調部は、逆スペクトラム拡散部から供給されてきた信号をGFSK復調し、得られたデータをベースバンド制御部607に出力する。

#### 【0104】

トランシーバ608は、2.4GHz帯を使用して、スペクトラム拡散が施された信号をアンテナ609から送信する。また、トランシーバ608は、アンテナ609からの受信信号を逆スペクトラム拡散部に出力する。

#### 【0105】

なお、ピコネットを構成する通信処理装置の各々は、図8に示したブルートゥースモジュール600と同様の構成を有するモジュールを備えており、上述の処理により各装置各のデータ通信を実行する。

#### 【0106】

上述したように、ブルートゥース規格に従った通信構成では、各機器はブルートゥースデバイス・アドレス（図9参照）という48ビットのIDを持つことが定められている。そして、このIDはブルートゥース規格に従った通信において、通信相手を特定するのに使用される。

#### 【0107】

通常、ブルートゥースデバイス・アドレスの情報は、図8を参照して説明したように、ブルートゥースモジュールのICに直接つながる不揮発性メモリ（フラッシュメモリ604）に書き込まれており、ソフトウェアなどで読み出すことはできるが、変更することはできない。

#### 【0108】

本実施例の認証シーケンスにおいては、ブルートゥースデバイス・アドレスを、2つの異なる方法で受信し、両者を比較して、一致すればローカル接続された機器間の通信、例えば同一のピコネットに接続された機器間の通信であると判定し、異なる場合には、外部ネットワークを介した通信であると判定する。

#### 【0109】

ブルートゥースデバイス・アドレスの取得処理は、以下の2つの取得処理によって取得したアドレスの比較を行う。

(1) 通信相手のブルートゥースデバイス・アドレスの情報をブルートゥース通信パケットのソースアドレスとして取得する。

(2) 例えば、2つの機器が共有する秘密鍵をもとにブルートゥースデバイス・アドレスを暗号化して伝送するプロトコルを決め、このプロトコルに従ってブルートゥースデバイス・アドレスを取得する。

#### 【0110】

このように、通信先デバイスの送信するパケットのソースアドレスとしてのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づく2つのブルートゥースデバイス・アドレスを取得し、これらの照合を実行する

。

## 【0111】

受信機器において、上記2つの方法で受信したブルートゥースデバイス・アドレスを比較して、一致すればローカル接続された機器間の通信、例えば同一のピコネットに接続された機器間の通信であると判定し、異なる場合には、外部ネットワークを介した通信であると判定する。

## 【0112】

ブルートゥース規格に従った通信を実行する機器同士で通信を行う場合、先に説明した図6(b)のように、機器Xが機器Cに、また機器Yが機器Aになりますことでブルートゥース通信範囲を超えた通信を行うことも可能である。これを防ぐため、機器Aは通信相手からきたパケットのソースアドレスとして入っているブルートゥースデバイス・アドレスと、前述の別のプロトコルによっても暗号などで保護されたブルートゥースデバイス・アドレスを取得する。

## 【0113】

この場合、ブルートゥースパケットのソースアドレスには機器Xのブルートゥースデバイス・アドレスが設定されており、機器Aと秘密鍵を共有する機器は機器Cなので、機器X、Y経由で機器Cのブルートゥースデバイス・アドレスを取得することになる。そして、これらのブルートゥースデバイス・アドレスの照合により、不一致が判明すると、機器Cがブルートゥースによるローカル通信領域、例えば同一のピコネットに存在しないと判定し、外部ネットワークに中継された通信を停止し、コンテンツ流出等の秘密情報の漏洩を防止することができる。

## 【0114】

上述したように、本発明の構成によれば、ホームネットワーク等のネットワークに対して、インターネット等の外部ネットワークに接続された機器からアクセスされた場合、そのアクセスが外部機器からか内部のローカルネットワーク内の機器からであるかを明確に判別することが可能となり、ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの漏洩、流出を未然に防止することが可能となる。

## 【0115】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

## 【0116】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

## 【0117】

例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory) に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magneto optical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

## 【0118】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインス

トールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

**【0119】**

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

**【産業上の利用可能性】****【0120】**

以上、説明したように、本発明の構成によれば、ホームネットワーク等のネットワークに対して、インターネット等の外部ネットワークに接続された機器からアクセスされた場合、そのアクセスが外部機器からか内部のローカルネットワーク内の機器からであるかを明確に判別することが可能となり、ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの漏洩、流出を未然に防止することが可能となり、コンテンツ著作権の管理の必要なコンテンツや、私的コンテンツ等、漏洩を防止することが必要なデータをローカルネットワーク内でのみ利用しようとするシステムにおいて適用されるデバイスで実行する認証シーケンスとしての適用が可能である。

**【図面の簡単な説明】****【0121】**

【図1】 ネットワーク構成例について説明する図である。

【図2】 通信処理装置の構成について説明する図である。

【図3】 IEEE1394 機器の構成について説明する図である。

【図4】 本発明の認証シーケンスについて説明するフロー図である。

【図5】 本発明の認証シーケンスについて説明するシーケンス図である。

【図6】 本発明の認証シーケンスによるID取得処理および効果について説明する図である。

【図7】 ブルートゥース規格による通信ネットワークについて説明する図である。

【図8】 ブルートゥースデバイスの構成について説明する図である。

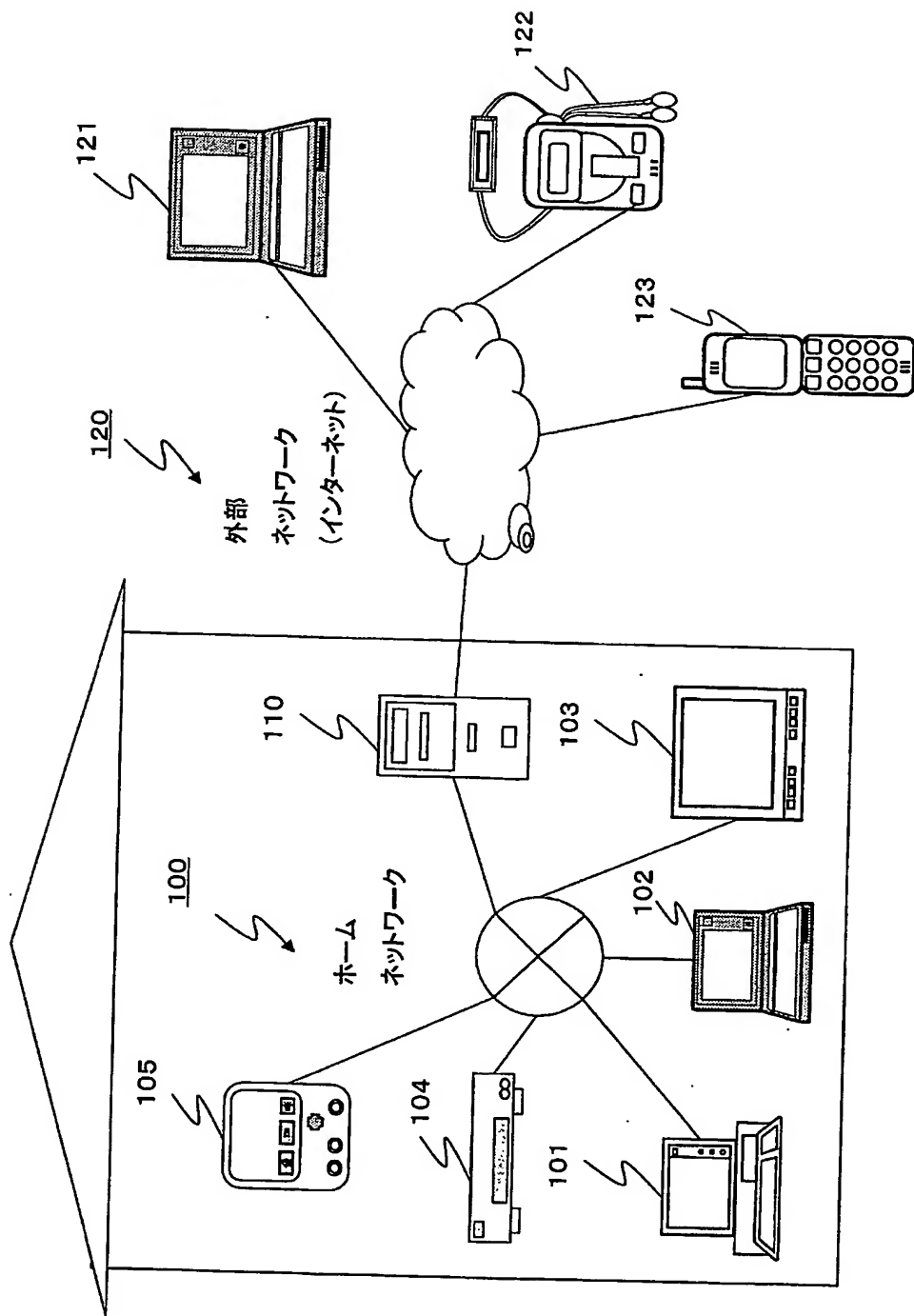
【図9】 ブルートゥースデバイスの通信において適用されるブルートゥースデバイス・アドレスの構成について説明する図である。

**【符号の説明】****【0122】**

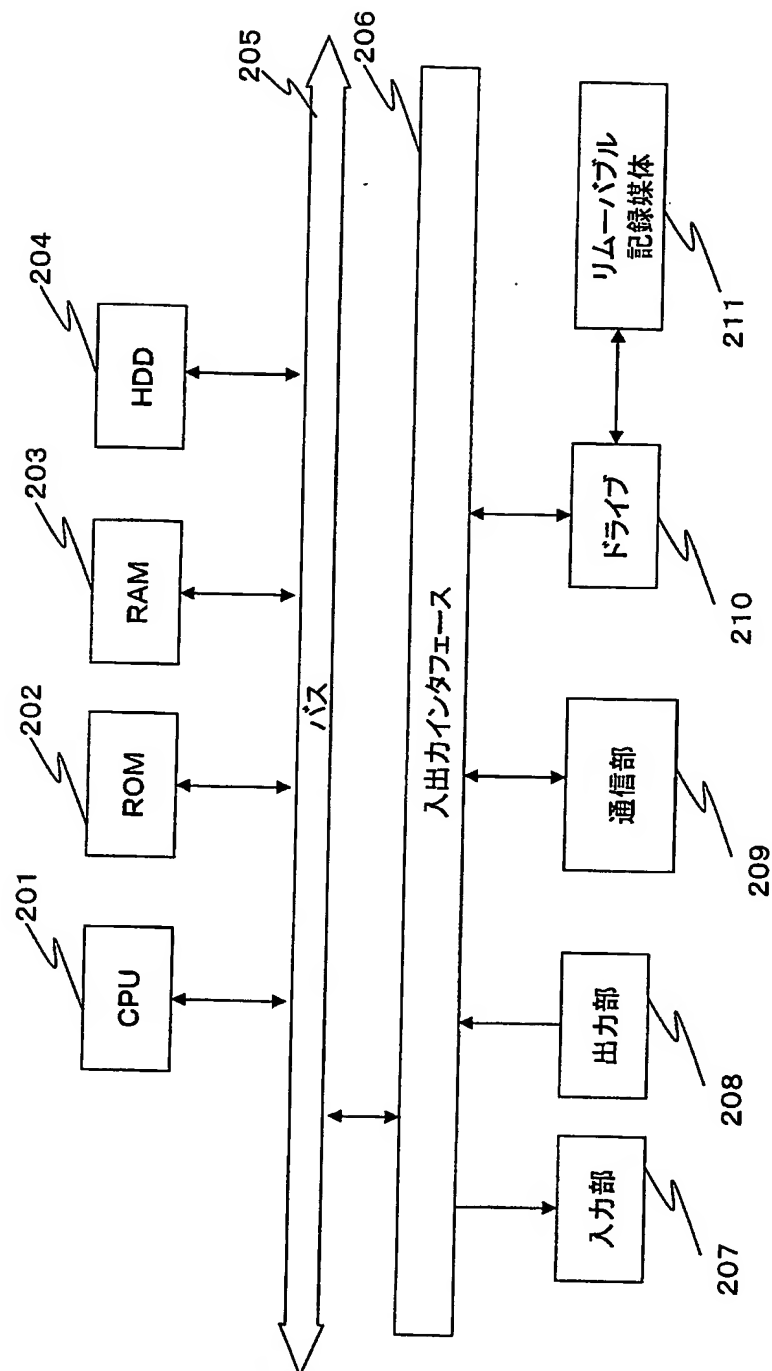
- 100 ホームネットワーク
- 101 PC
- 102 PC
- 103 TV
- 104 ハードディスクレコーダ
- 105 PDA
- 120 外部ネットワーク
- 121 PC
- 122 携帯電話
- 123 ポータブル再生プレーヤ
- 201 CPU (Central Processing Unit)
- 202 ROM (Read Only Memory)
- 203 RAM (Random Access Memory)
- 204 HDD (Hard Disk Drive)
- 205 バス
- 206 入出力インタフェース

- 207 入力部
- 208 出力部
- 209 通信部
- 210 ドライブ
- 211 リムーバブル記録媒体
- 301 送受信部
- 302 IEEE1394 端子
- 303 PHY-IC (PHY通信部)
- 304 LINK-IC
- 305 ネットワーク通信部 (IEEE1394 制御マイコン)
- 306 機器制御マイコン
- 310 1394 バス
- 411 機器A
- 412 機器B
- 421 機器A
- 422 機器C
- 431 機器X
- 501 パーソナルコンピュータ (PC)
- 521 パーソナルコンピュータ (PC)
- 522 携帯電話
- 523 PDA (Personal Digital Assistants)
- 524 ビデオカメラ
- 600 ブルートゥースモジュール
- 601 CPU
- 602 ROM
- 603 RAM
- 604 フラッシュメモリ
- 605 バス
- 606 入出力インタフェース
- 607 ベースバンド制御部
- 608 トランシーバ
- 609 アンテナ

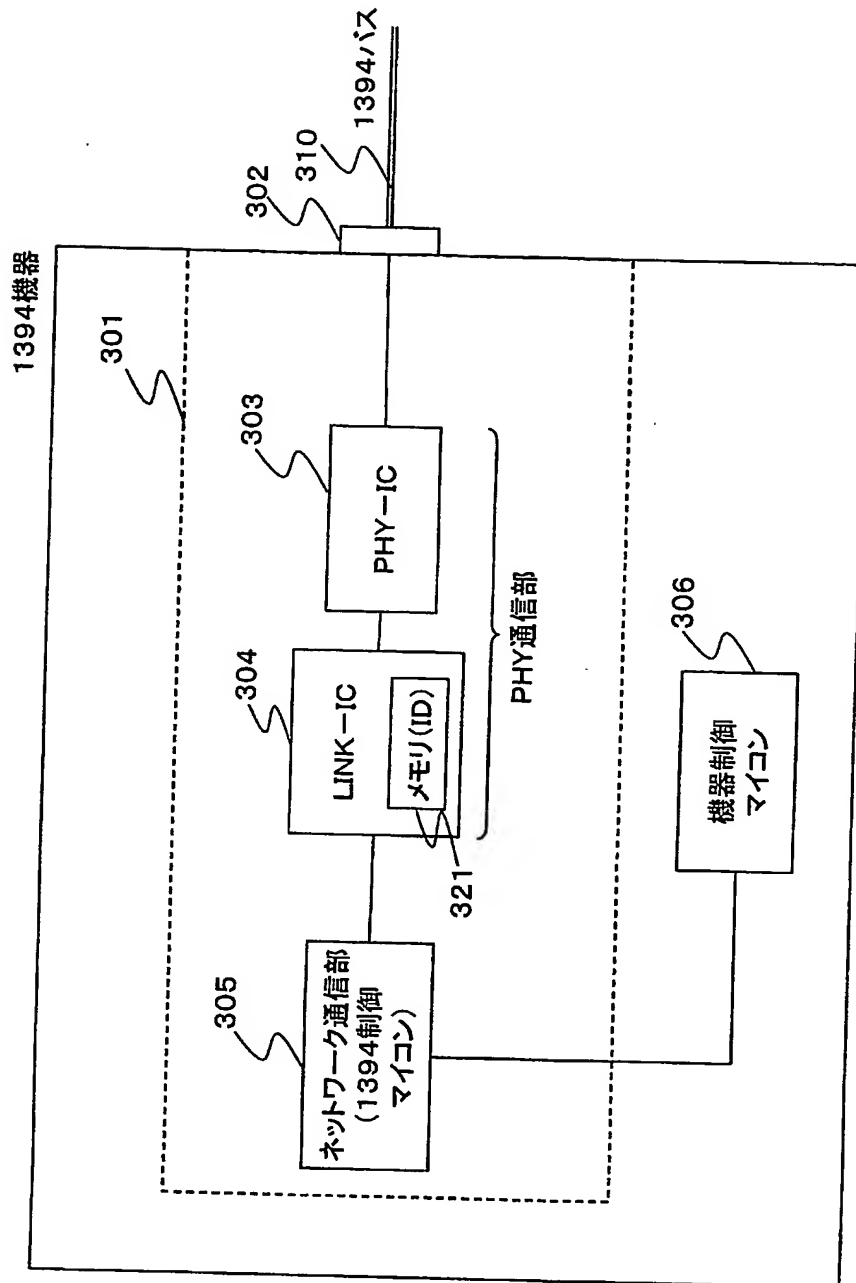
【書類名】図面  
【図 1】



【図 2】

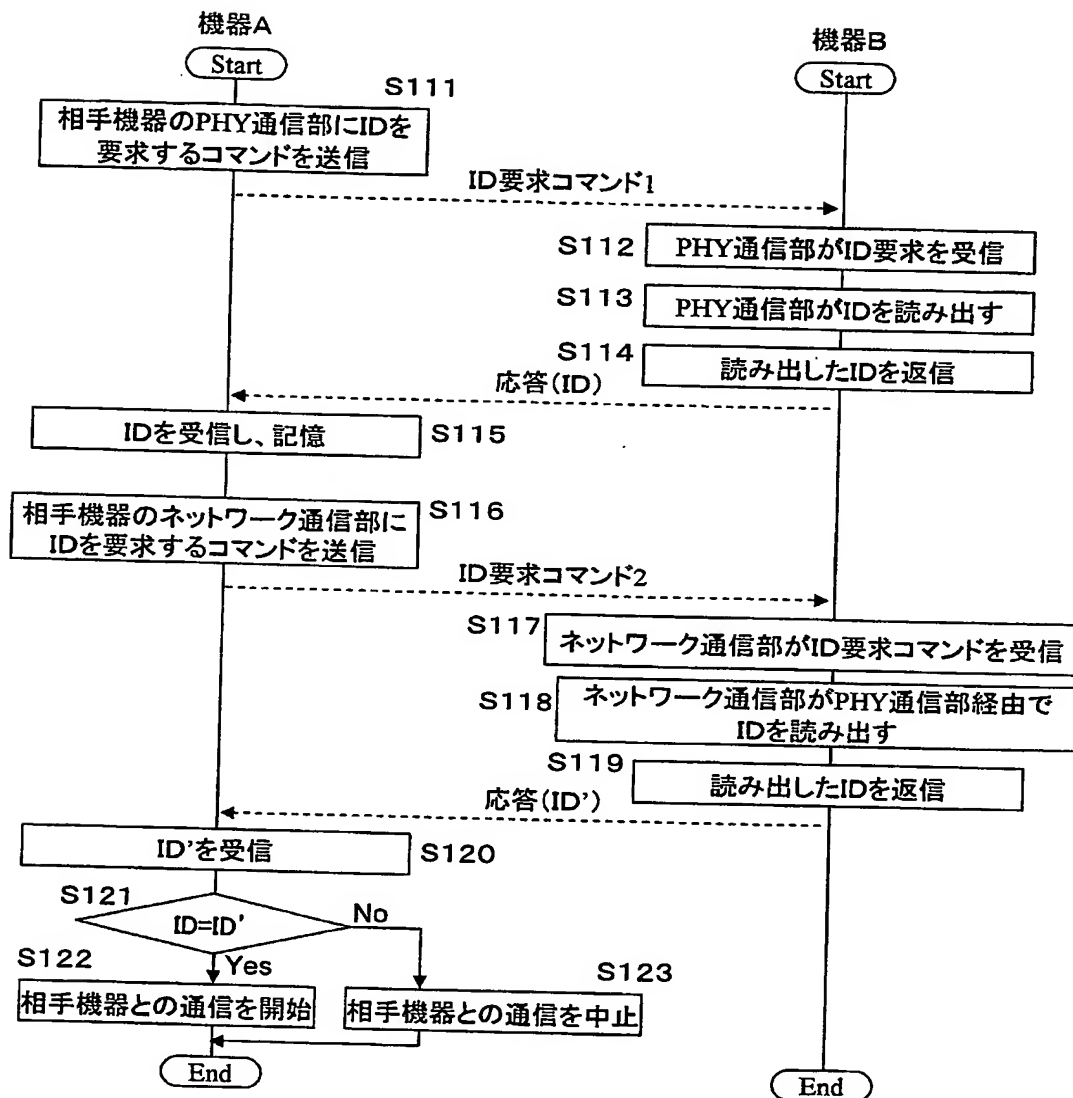


【図 3】

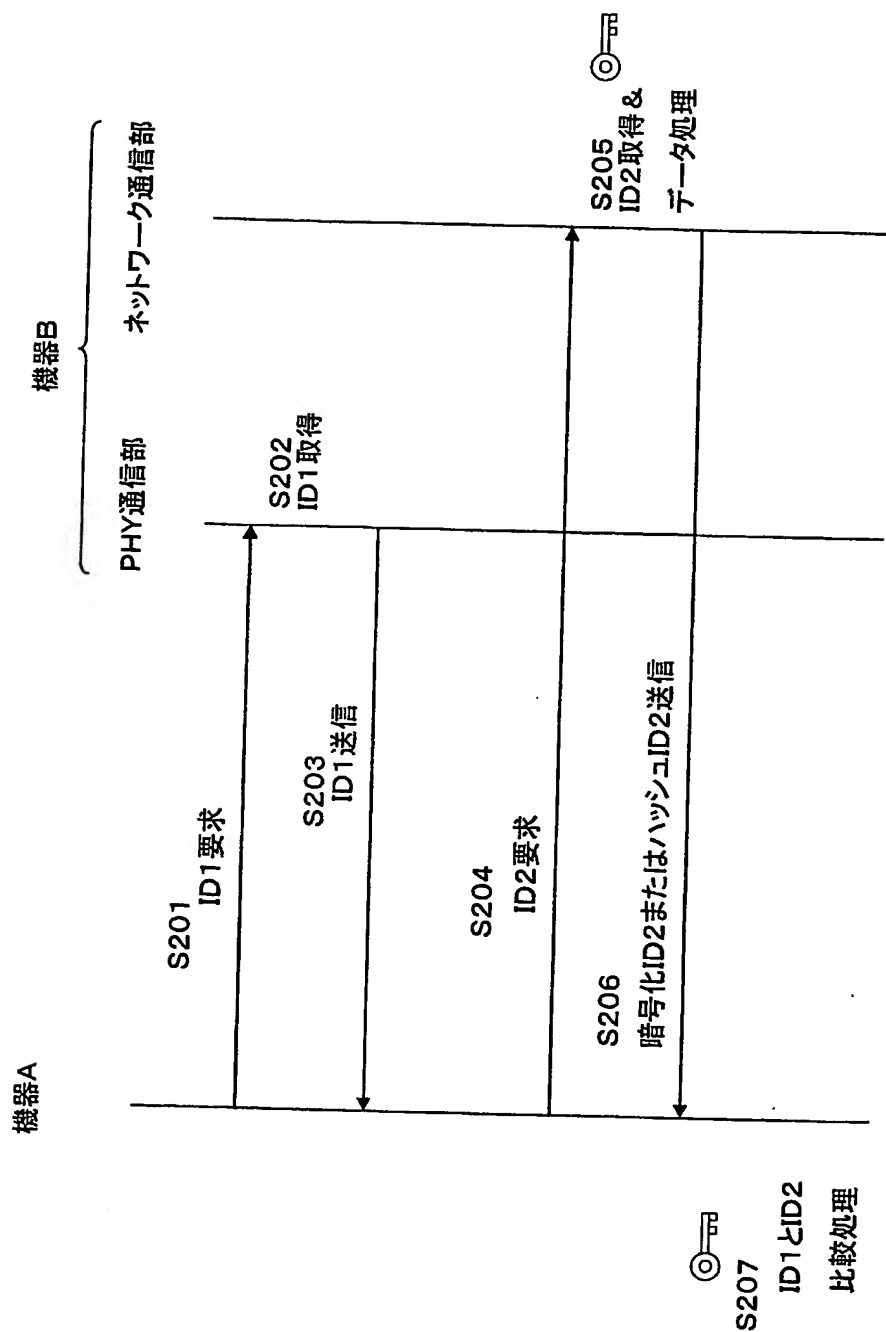




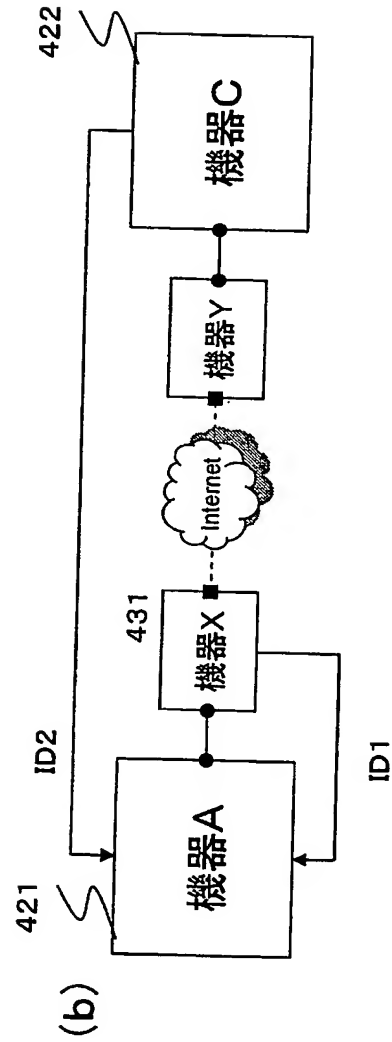
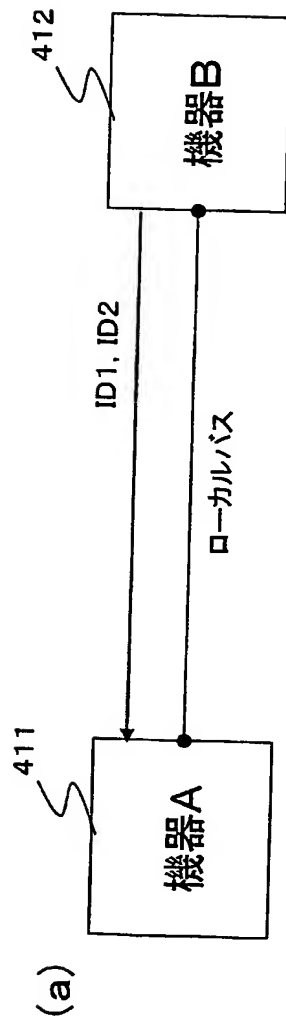
【図4】



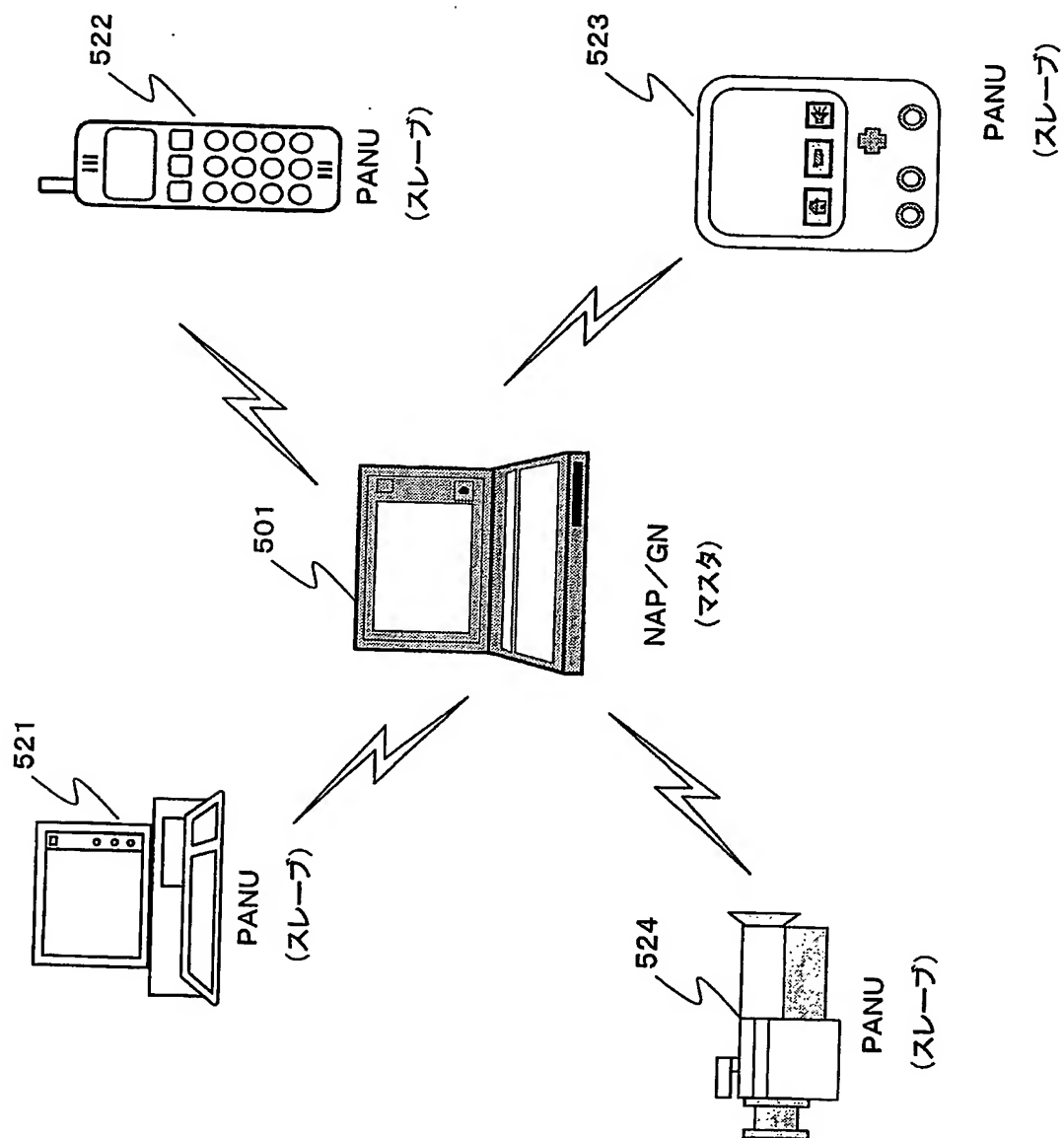
【図 5】



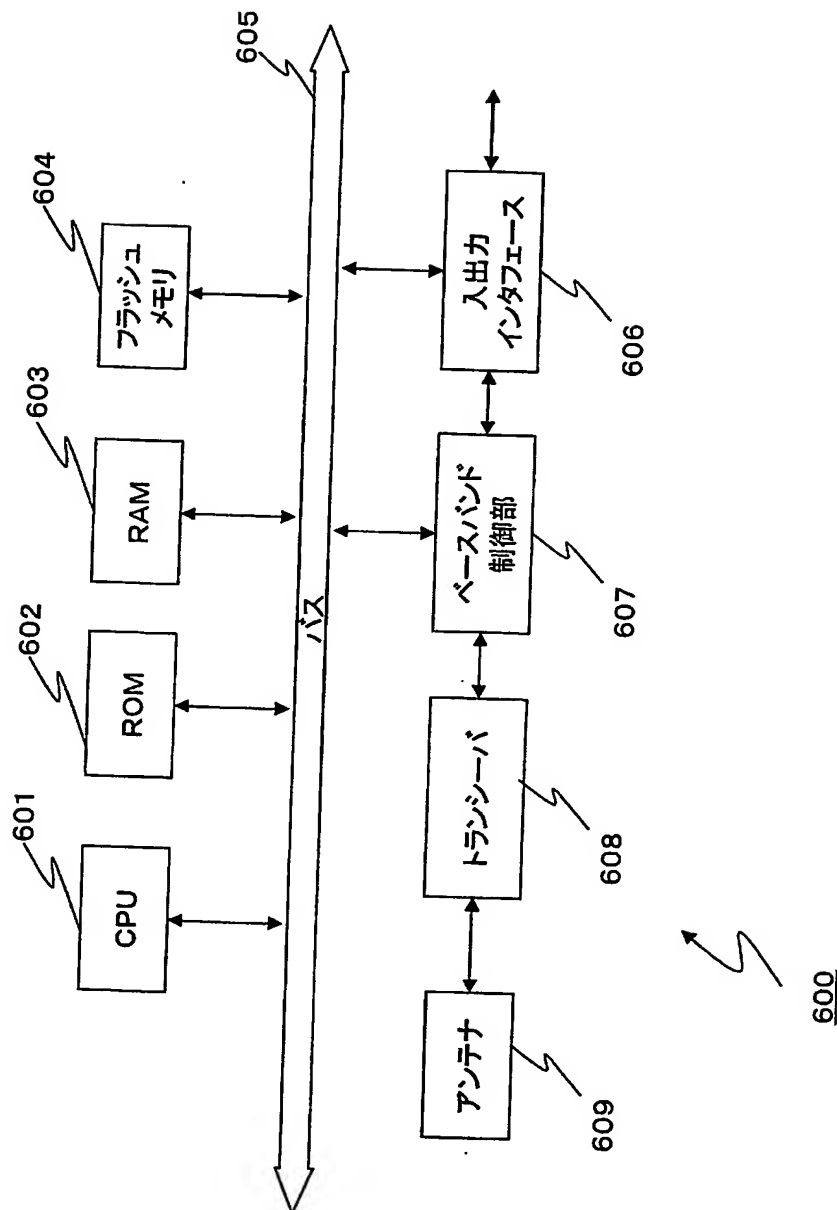
【図 6】



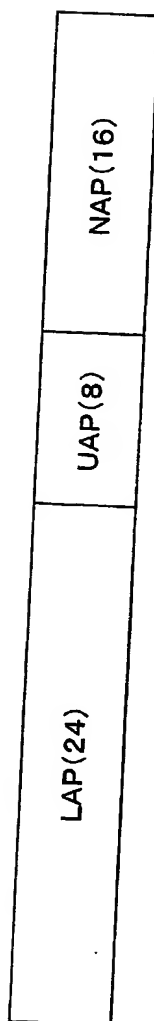
【図 7】



【図 8】



【図 9】



【書類名】要約書

【要約】

【課題】 ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの外部に対する漏洩、流出を未然に防止することを可能とした構成を提供する。

【解決手段】 通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する。例えばOSI参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信し、これらの識別情報の照合を行う。また、少なくとも1つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成による生成データを受信する。複数の識別情報の照合を行い、照合の成立または非成立に基づいて、通信先デバイスが同一のローカルネットワークに接続されたデバイスであるか否かを判定する。

【選択図】 図5

特願2003-291971

出願人履歴情報

識別番号

[000002185]

1. 変更年月日  
[変更理由]

1990年 8月30日

新規登録

住 所  
氏 名

東京都品川区北品川6丁目7番35号  
ソニー株式会社



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**